eurelectric
powering people

ENTSO-E & EU DSO Entity consultation on Cybersecurity Network Code

A Eurelectric response paper

December 2021

Eurelectric represents the interests of the electricity industry in Europe. Our work covers all major issues affecting our sector. Our members represent the electricity industry in over 30 European countries.

We cover the entire industry from electricity generation and markets to distribution networks and customer issues. We also have affiliates active on several other continents and business associates from a wide variety of sectors with a direct interest in the electricity industry.

We stand for

The vision of the European power sector is to enable and sustain:

- A vibrant competitive European economy, reliably powered by clean, carbon-neutral energy
- A smart, energy efficient and truly sustainable society for all citizens of Europe

We are committed to lead a cost-effective energy transition by:

investing in clean power generation and transition-enabling solutions, to reduce emissions and actively pursue efforts to become carbon-neutral well before mid-century, taking into account different starting points and commercial availability of key transition technologies;

transforming the energy system to make it more responsive, resilient and efficient. This includes increased use of renewable energy, digitalisation, demand side response and reinforcement of grids so they can function as platforms and enablers for customers, cities and communities;

accelerating the energy transition in other economic sectors by offering competitive electricity as a transformation tool for transport, heating and industry;

embedding sustainability in all parts of our value chain and take measures to support the transformation of existing assets towards a zero carbon society;

innovating to discover the cutting-edge business models and develop the breakthrough technologies that are indispensable to allow our industry to lead this transition.

Dépôt légal: D/2021/12.105/57

WG Technology
DSO Experts Group on Cybersecurity

Contact:
Caoimhin O'BRIAIN, Senior Advisor - Distribution & Market Facilitation – cobriain@eurelectric.org

Title I: GENERAL PROVISIONS

7. Are the objectives of the Network Code on Cybersecurity, which lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management sufficiently clear?

○ Yes ○ No opinion ◉ No

If your answer is "No", please elaborate

A lot of work and requirement for actions is left to ENTSO-E, EU-DSO, ENISA and ACER with the support of national authorities to develop as well as to decide. Stakeholders like generators and suppliers are not typically represented in EU-DSO or ENTSO-E groups. Should the cybersecurity working group described in Art 15(1) be retained we would ask for a broad inclusion of stakeholders and a better definition of (i) rules of governance and (ii) selection process for stakeholders' representatives.
Further clarity is required on the definition of cross-border electricity flows and the framework for the deliverables of the Working Group, as these parameters have a big impact on the scope of the network code.
It may be easier to comment on the network code if we understood what the cybersecurity working group would consider an ECII threshold for example for generators in terms of MW of production before being deemed high risk.
As a general comment, it is key to ensure that the objectives of the NCCS and of the NIS 2 Directive are correctly aligned.

Art 3(1)(a) to (k) proposes objectives which are dissimilar in nature and importance, and could be reordered for a clearer outcome:

- More emphasis should be put on the objective of ensuring the cybersecurity of the entire electricity system from end to end. This would include the operational security of cross-border flows, and of the entire system (in line with art.4 of System Operation Guidelines (SOGL - Regulation 2017/1485), which focuses on the operational security of the system).
- Given the high number of objectives (11), some could be merged, and others deleted (e.g. monitoring is not as such an objective but rather a tool to ensure the efficiency of the NCCS).

In the text "Regulatory authorities" are mentioned without explanation in Article 3 Objectives. Is it still a role / function, or should it read competent or national regulatory authorities? Legal experts should check that the correct role is defined in the text for the correct division of responsibilities.

8. The NCCS states: "Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation." Based on the statement above, are twelve months a reasonable timeframe?

○ Yes ○ No opinion ◉ No

If your answer is "No", please elaborate

Small sized companies have no ISMS competence on their payroll and must undertake large projects with external consultants to clear up their OT service management and information security management.

We suggest at least 18-24 months for implementation. Together micro and small sized entities could have an impact on the cross border cyber security. It is important to identify critical/essential business processes even for small DSOs to perform the risk assessment at least in the level 1 (local). In legacy contracts this depends on the Service Providers and may last longer than 12 months. Within 12 months the process to renew the contracts to include Cyber Security must be started.
It may depend whether there are critical technology impacts like changes to intelligent electronic devices. In such cases a much longer transition period is required. We propose minimum 18-24 months as above.

It is noted that Annex A provides a list of very light requirements which may already be implemented by many entities irrespective of their size.

9. The NCCS states: "Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation." Based on the statement above, do you think these requirements for small and micro enterprises are of sufficient level?
○ They are too strict ○ They are at the approproate level ◉ No opinion ○ They are too flexible, more strict requirements should be in place
If your answer is "They are too strict" or " They are too flexible, more strict requirements should be in place", please elaborate

10. Do you consider the Monitoring approach defined at Article 12 to be effective to monitor the adequacy of the Network Code to the ever-changing technology landscape and evolution of applicable cybersecurity standards?
○ Yes ○ No opinion ◉ No
If your answer is "No", please elaborate

We welcome the proposed art.12 on monitoring in that sense that it aligns to a great extent with the monitoring articles which can be found in other NCs and GLs. We note a certain confusion in the allocation of responsibilities between ACER and the so-called Monitoring Body. Whereas art.12.2 seems to vest ACER with the responsibility to evaluate the adequacy of the NCCS, the Monitoring Body would be vested by art.16.2 with the responsibility of monitoring the implementation of the NCCS and its methodologies. We believe that all those activities should be clearly allocated to ACER, in art.12. To perform this monitoring, ACER could organise a consultation with other public authorities, therefore removing the need for a Monitoring Body in the framework of this NC.

If each entities use different risk description, the aggregation to member state is quite complex. The monitoring does not describe the process to go back to the previous normal system.

Too many updates may cause hinderance. Every two years or less frequently is appropriate since the principles can remain unchanged for several years.

11. Do you think the Benchmarking approach, as described in Article 13, is an adequate tool to assess whether current investments in cybersecurity to protect cross-border electricity flows are sufficient?
○ Yes ○ No opinion ◉ No

If your answer is "No", please elaborate

The intention to create a benchmark is good, despite the result of the analyses in combination with business analysis may create great differences between regions and within Member States which may result in distorted competition between Member States.
In the current proposal, the added value of the NRAs/CS NCAs collecting information on cybersecurity costs is not apparent. Although the proposed approach could provide NRAs with a good overview of cybersecurity costs and their global efficiency, this would not strengthen cybersecurity until:

- the entities participating in the benchmark are informed and therefore can compare their practices with each other. The information process for entities must be mentioned or proposed.
- best practices are shared (equipment, tools, processes, ideas)

The current proposal seems to be a burdensome process with limited practical use and unclear objectives. It may therefore be better for public authorities to keep supporting the voluntary exchange of best practices between actors of the sector, in the respect of competition law rules.

The proposal is expensive and difficult to implement. It is difficult to analyse the correlation of cybersecurity investments to expected results.

12. Do the overall timelines within the Network Code on Cybersecurity seem reasonable?
○ Yes ○ No opinion ◉ No
If your answer is "No", please elaborate

The overall calendar seems quite ambitious. Too tight a schedule can lead to security issues. Most of the deadlines are packed in a two-year assessment cycle: i) definition high impact or critical impact entity, ii) definition of the minimum and advanced controls, iii) possibility to obtain a derogation; iv) obligation to comply with the controls and v) obligation to demonstrate compliance with these controls.

This comes in addition to the obligations to perform the risk assessments, participate in two cybersecurity exercises on a three-year basis, implement plans for the update of legacy systems, etc.

Apart from the multiplicity of obligations, the apparently conflicting timelines lead to a situation where it cannot be easily determined at any point in time i) who are the subject of the obligations and ii) what are the nature of their obligations. This could lead to a suboptimal (or even no) implementation of and compliance with the NCCS.

The timelines (2Y) differ from the timelines in NIS-directive and in member states (3Y), which may create conflicts with national laws and will give at some milestones “old” information.

The Energy sector face multiple new targets for managing controls and meeting new security requirements that must be coordinated both by EU and in a national manner by authority according to requirements as the up-coming NIS-2 and Cybersecurity Act as well as this new regulatory instrument. The regulations must be coherent and streamlined to each other as far as taxonomy and methods are concerned.

Respecting due dates depend on the efforts related to, for example, the complexity of the methodologies and measures (minimum and advanced) mapped into ECSMM (still undefined) so it is not possible at this stage to fully evaluate this topic and hence to fully answer the question.

Title II: GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

13. Is it reasonable that the entities involved can perform the following tasks within the time set in the network code, given resource, capability, or other constraints? Activities led by the CS-NCA and NRA: a) CS-NCA and NRA to perform the member state risk assessment within 3 months (Article X) b) CS-NCA and NRA to make a transitional list of high-impact and critical-impact entities within 6 months after receiving the transitional ECII (Article Y) c) CS-NCA and NRA to identify high-impact and critical-impact entities within 6 months after receiving the ECII (Article Z) Activities performed by entities: d) High-impact and critical-impact entities to report the results of their risk assessment in 6 months e) High-impact and critical-impact entities to implement the minimum and advanced cybersecurity controls in 6 months after their publication f) High-impact and critical-impact entities to provide evidence of verification of the controls in 24 months after their publication

○ Yes ○ No opinion ◉ No per activity

Do you have any additional comments on the timelines

There is a significant increase in the number of obligations allocated to CS-NCAs and NRAs, which will require increased time and resources.

With regard to activities led by electricity entities, there are still too many tasks involving a great number of stakeholders to realistically fit within a 2-year cycle. As an alternative, we recommend longer risk assessment cycles or a simplification of the corresponding workflows. The latter might be the only practical outcome should we want to keep the pace with the fast-changing technology. In practice, with the current proposal:

- Risk assessment: the timeline is too short, especially for the first round of risk assessment;
- Compliance with the minimum and advanced cybersecurity controls: we cannot say whether the timeline is appropriate as we do not know what those controls will be;
- Provision of evidence of the controls: it is too early to assess whether 24 months would be sufficient for verifying the compliance with controls.

High impact entities should be allocated more time for reporting and implementation.
Establishing the network code is time consuming process. Thus, careful implementation should be facilitated by allowing more time for the process.
The timeframe for CS-NCAs and/or NRAs to analyse national legislation and to identify high-impact and critical-impact entities is far from adequate. This means entities risk a low quality in the matrix mentioned in article 25 and the identification mentioned in article 27, and thereby an arbitrary implementation.

Furthermore, the current timeframe does not consider that more time will be needed to define national responsibilities between government agencies. Responsibilities within energy, NIS, cyber security, and national security are not totally aligned and might need legislative adjustments on a national level. This is crucial for a quick and efficient implementation process at entity level.
Respecting due dates depend on the efforts related to, for example:

- the granularity of Critical / High processes defined by ENTSO-E and EU DSO Entity;

- the complexity of the methodologies and measures (minimum and advanced) mapped into ECSMM (still undefined) so it is not possible at this stage to correctly evaluate this topic and hence to fully answer the question.

14. Is the proposed governance for cybersecurity risk assessment clearly described and sufficient to meet the objectives of the network code on cybersecurity?

○ Yes ○ No opinion ◉ No

If your answer is "No", please let us know what could be improved?

The proposed governance for cybersecurity risk assessment is not clearly described and sufficient.

The risk assessment methodology is too vague, especially regarding the intended content of the risk assessment methodology and the specificities which would apply depending on the geographical level (Union, regional, national or entity level) of the risk assessment.

Should the cybersecurity risk working group be maintained, high-impact and critical-impact entities should have a bigger role in it. If the scope of the network code is to be expanded, this should be reflected in the governance. Otherwise, parts of the sector would be governed by a too narrow group. Please define what will the ECII high and critical thresholds be in practice or further details on the parameters to be considered and the meaning of the level of impact on the power system.
The compliance is typically enacted to protect information systems and sensitive data. However, they frequently evolve to promote equal competitiveness between Member States according to information technology, industry influences and new threats to systems and data. We propose an approved national methodology for risk assessments for clarification of critical processes for the OT environment for increased delivery security. We also see need of clarification on security requirements for especially OT-processes.

Title III: RISK MANAGEMENT AT UNION AND REGIONAL LEVEL

15. Under the network code draft, cybersecurity risk assessments are performed at four levels: Union-wide, regional, member state, and entity. By integrating information from these four levels, it should be possible to get a comprehensive view on the risks. How effective do you think this multi-level process will be in assessing and reducing the cross-border cybersecurity risks in the European electricity sector?

○ Very ineffective ○ Ineffective ○ No opinion ◉ Effective ○ Very effective

If you think the process is not effective, how can it be improved?

How do you think the efficiency of the risk assessment process could be improved?

Each level should limit the information shared to a need-to-know principle, in an aggregated manner.

Merging the Union and regional risk assessments could be considered to streamline the process, as their input and deliverables, the methodology and the actors involved are very much the same.

We believe it is important to set requirements based on functionality and processes. Our concern is that rules on cybersecurity will be defined in the network code, but its scope of applicability will

remain unclear until either (i) development and implementation of a methodology on risk assessment and defining Electricity Cybersecurity Risk Index (ECRI) or (ii) transitional measures are adopted by the cybersecurity working group. This representants significant uncertainty for the electricity undertakings.

Provide simple and easy to use templates in advance. We suggest to avoid increasing complexity. In particular, we suggest to define harmonized tools and metrics to correcly manage the four different levels of Risk Assessment (for example, clear and homogeneus Impact Matrix, Threats, etc.) without causing added effort to entitites that already have their methodology.

16. The proposed scope of the cybersecurity risk assessments is the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. Legal, financial or reputational damage of cyber-attacks are out of scope. Do you think this is a good scope to manage the cybersecurity risks to cross-border electricity flows?

○ Yes ◉ No opinion ○ No

If not, what should be added to or removed from the scope?

17. Under the proposed cybersecurity risk management process, ENTSO-E and EU DSO with the RCCs make and approve a risk treatment plan. In approving the plan, they could be seen to accept the residual risks. Do you think this is an appropriate process for accepting the residual risks?

○ Yes ○ No opinion ◉ No

If not, which party should be responsible for accepting the residual risk at regional level?

If the requirements in the network code are mandatory, an approval step is required at European level to independently rubber stamp the risk treatment plan. The network code sets minimum requirements and does not prevent national authorities or entities going above these minimum requirements. After the approval at regional level, national regulatory authorities could still elect to adopt more stringent requirements and therefore lower further the acceptable level of cybersecurity risk in their country.

We understand, however, that by virtue of art 5.5 the remedial risks identified in the regional risk treatment plan are accepted by the approval of all the relevant NRAs at regional level. This seems to be a better approach as it puts the regulatory authorities in a position to evaluate the acceptable level of cybersecurity risk.

18. Is the proposed risk management at union and regional level clearly described and sufficient to meet the objectives of the network code on cybersecurity?

○ Yes ◉ No opinion ○ No

If your answer is "No", what could be improved?

Title IV: COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

19. Are the minimum cybersecurity controls for supply chain security in Article 24 (2) clear and sufficient?

○ Yes ○ No opinion ◉ No

If not, how should they be amended?

There is an inconsistency between Article 35 and 24. In Art 24, the harmonised procurement requirements and the procurement requirement defined by the entities are described as alternatives. Yet, we understand that the first ones are meant to describe technical parameters applicable to products or services whereas the later (and the list of points i) to ix) in Art 24(2)(a)) are meant to apply to the procurement process itself.

It is therefore unclear whether the points i) to ix) of Art 24(2)(a) should be part of both the harmonised procurement requirements and the procurement requirements established by the entities and whether they would apply from the applicability date of the NCCS.

In any case, it seems important for the drafting team to consider further the impact of the definition of new procurement requirements in case of procurement framework contracts. The NCCS doesn't consider the industrial reality of electricity entities:

- What is the impact of the procurement requirements on multi-year industrial purchase programs? Please consider how in certain circumstances, the NCCS could authorise electricity entities to purchase the same equipment before & after the entry into force of the procurement requirements to ensure the continuity of procurement strategy.
- The creation of a new ICT product may require several years. The NCCS should take into account the need of the industrial actors to know in advance how the procurement requirements will evolve. Consequently, the rolling work program should be known in advance.

We therefore invite the drafting team to review the interplay of Art 35 and 24, the applicability of the points i) to ix) of Art 24(2)(a) and to propose an alternative which takes into account the impact of the adoption of procurement requirements on existing procurement framework contract.

We propose voluntary certification on essential products and not mandatory requirements. Product and measurements certifications are very farfetched and may potentially result in limiting the availability of ICT products on the market and restrain innovation. At the same time, the measures foreseen by the FG do not include measures that are easier to apply: introducing basic level of security for services and products, long-term security patches or standard contractual clauses that would improve the situation of electricity undertakings vis-à-vis the vendors.

It is missing how to deal with existing contracts around legacy systems operation and MRO.

The process for procurement requirements must be very clear and transparent - this is an arena for pressure from both suppliers and nations. Here, the EU's competitiveness and free market must be safeguarded.

20. The supply chain controls now require entities procuring new products and systems to set and enforce security requirements to suppliers. Should the network code also include controls that directly require suppliers to take certain measures?

(●) Yes ( ) No opinion ( ) No

If your answer is "Yes", please write what measures should be required from suppliers

An obligation should indeed be established directly on the suppliers providing goods or services to an electricity entity. This would ensure that the supplier is invested in the cybersecurity of the

products and services it supplies and, consequently in the cybersecurity and operational security of the electricity system as a whole.

The obligation would move the topic of cybersecurity from an issue of contractual negotiations between parties of different strengths to an issue of compliance of the parties with their legal and regulatory obligations.

It is noted, however, that without suppliers involved in the discussion such requirements may be difficult to enforce. Suppliers must be on board.

21. The network code proposes cybersecurity hygiene requirements in Annex A to ensure that all entities that can affect the cybersecurity of the electricity grid have a baseline security. Do you think the proposed hygiene requirements are appropriate for reducing cross-border cybersecurity risks?

○ Yes ○ No opinion ◉ No

If your answer is "Yes", please write how should the requirements be rephrased

We support the idea of hygiene requirements but it should be considered carefully in which legal instrument they should be included. The entities subject to these hygiene requirements do not (as demonstrated by the high and critical ECII thresholds) contribute to security of cross border electricity flows, and so could be considered outside the remit of the network code. Their removal or changing their nature to advisory only should be considered, especially given the revisions ongoing to the NIS directive which may already now include hygiene requirements.

The scope of entities subject to these requirements are small and micro enterprises excluding those that were classified as high or critical by NCAs, as per article 2.3. It is noted that the second paragraph of Annex A appears to contradict this which may be a source of confusion.

Please define also what will the ECII high and critical thresholds be in practice.

22. Is the proposed common electricity cybersecurity framework clearly described and sufficient to meet the objectives of the network code on cybersecurity?

○ Yes ○ No opinion ◉ No

If your answer is "No", please write what could be improved

It is not possible to provide a complete answer to this question, as most of the information required will be provided later:

- Business processes are unknown
- ECII will be developed later (high-impact / critical-impact threshold)
- Controls are not defined yet
- National frameworks to be used will be determined later

Title V: RISK MANAGEMENT AT MEMBER STATE LEVEL

23. CS-NCA and NRA can appoint entities as high-impact or critical-impact even where they do not individually meet the ECII level. This allows them to appoint entities for which the aggregate impact

of a group of similar entities is above the high-impact or critical-impact thresholds. Do you agree with this mechanism for dealing with groups of similar entities?

○ Yes ○ No opinion ◉ No

If not, what mechanism should be used to deal with groups of entities?

This mechanism is a very good starting point. However, the description carried out to identify these entities remains to the evaluation of the CS-NCAs without any methodology: the NCCS should provide methodologies to assess this type of risk and not leave a "may" with excessive application hazards according to the understanding or the sensibility of each country. A clear, objective and reliable process needs to be established instead.

We understand from the FG that the NC should be reorganised so as to ensure that there should be:

- 3 categories of electricity entities: critical impact entities, high impact entities and SMEs. SMEs would fall under the scope of the NCCS even though they would only be required to comply with the hygiene requirements;
- A possibility for the CS NCAs to reclassify an entity at a higher level if it meets the ECII threshold. In this way, an SME would already fall into the scope of application and could be asked to comply with the obligations of a high impact or critical impact entity if it meets the criteria defined in the ECII threshold.

The ECII threshold could be designed to contain a criterion where a coordinated cyberattack against multiple similar entities could lead to a significant impact on the operational security of the electricity system and/or cross-border electricity flows. NB: aggregators do fall in the scope of the NCCS and it is already possible to define a threshold for aggregators.

24. Is the proposed risk management at member state level clearly described and sufficient to meet the objectives of the network code on cybersecurity?

○ Yes ◉ No opinion ○ No

If your answer is "No", what could be improved?

Title VI: RISK MANAGEMENT AT ENTITY LEVEL

25. In Article 31, the network code requires entities to report information about existing controls, threats and vulnerabilities to their national regulators (CS-NCA and NRA). The regulators then report this information to ENTSO-E and the EU DSO entity for the regional risk assessment (Article 26). The information will give a good and detailed view of the cybersecurity risks to cross-border electricity flow. But the information could also be exploited by potential threat actors if they could obtain it. Do you think the benefit of collecting the information will be large enough to outweigh the risk of the information being compromised?

○ Yes ○ No opinion ◉ No

If your answer is "No", what changes would you propose?

At the moment, the mechanism whereby the information is collected from the entity level and transmitted successively from the national to regional to EU wide level is not clear and apparent.
The bottom-up approach of collecting information is welcome, but there is no obvious need for this level of granularity of data to be reported that high up. It creates more risks for the detailed information to be seized by cyber pirates and used against the electricity entities. The network

code should adopt the need-to-know principle and only share aggregated and anonymised information with the higher level in order to limit risks. By sending a summary of threats and vulnerabilities, electricity entities realise a first aggregation.

There should also be specific cybersecurity requirements on those collecting this information to avoid any unintentional disclosure of data.

The information collection induces too high a risk for leakage, or the information won't give enough knowledge for deducing an assessment of adequate quality.
The transmission part should not be forgotten (encrypted communication) at national level exchanges, where sensible data may be sent.

26. Entities determine the scope of the entity level risk assessment based on the outcomes of the Union-wide risk assessment, in particular the list of Union-wide high-impact and critical-impact processes. Do you think the process for determining the entity-level risk assessment scope is clear, and that the scope will cover all assets the entity needs to support cross-border electricity flows?
○ Yes ○ No opinion ◉ No
If not, how can the scoping of the entity-level risk assessment be improved?

The list of critical-impact / high-impact processes is needed to properly answer this question.

With regards to the risk management at entity level, Art 29 proposes to bring together in a single article all aspects related to context establishment, cybersecurity risk assessment, risk treatment and risk acceptance. Those aspects have been treated in different, autonomous Articles for the Union level, regional level and national level. The reason justifying such a difference of approach (integrated approach vs. split up approach) is not clear.

The interplay of the risk management at entity level with the risk assessments and their deliverables at Union, regional and national levels is not apparent in the draft NCCS.

With regards to Art 29(3)(a), we understand that the scope of the cybersecurity risk assessment is to be defined in relation to the high impact and critical impact processes identified in the report of the pan-EU risk assessment in Art 19(2)(a). The exact interplay between those two is nevertheless unclear and should be clarified if we want to ensure a coherent and harmonised implementation of the NCCS across the EU and therefore an increased level of cybersecurity in the EU.

Finally, it must be noted that, as the scope of the cybersecurity risk assessment for the electricity entities is to be defined in relation to another deliverable of the NCCS which is out of their controls, it is impossible for electricity entities to know in advance the exact scope of their cybersecurity perimeter and what efforts they would have to make to comply with their obligations stemming from the NC CS.

It is important to identify critical/essential business processes even for small DSOs to perform the risk assessment at least in the level 1 (local).

27. The network code allows the CS-NCA and NRA to give derogations based on three criteria: (a) in exceptional circumstances, when the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefit; (b) The entity can provide a risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is

acceptable according to the risk acceptance criteria pursuant to Article 25.3.b. The risk treatment plan shall be verified through one of the options pursuant to Article 33. (c) The results of the risk assessment of the entity do not show any direct or indirect impact on cross-border electricity flows. Do you agree with the criteria and process for providing derogations?

○ Yes ○ No opinion ◉ No

If not, how can the derogation process be improved?

With regard to the process followed for granting derogations, several modifications are required to streamline and increase the robustness and efficiency of the process:
a) there should be only one entity in charge of granting the derogation;
b) a deadline for granting the derogation should be inserted in Art 30, so that both the requester and the public authority can rely on an expected timeline;
c) the process needs to be streamlined so that electricity entities can quickly benefit from derogations and can then focus their efforts on complying with their obligations.

With regard to the conditions listed for the derogation, we believe that they need to be further worked upon to ensure their legal robustness and make sure that the view of the electricity entities plays a proportionate part in the assessment of the derogation requests:
(a) on condition A: against which objective criteria do we evaluate that the costs exceed the benefits? And what if the costs are very important but that there is still a great benefit for the entire system? Are the benefits to be assessed for the electricity entity or for the system?
(b) on condition C: by definition, the obligations for which a derogation is sought are applying to high impact or critical impact entities (minimum and advanced cybersecurity controls), which means that those entities are deemed to have an impact cross-border. How could a risk assessment therefore demonstrate that there is no impact cross border?

28. Is the proposed risk management at entitiy level clearly described and sufficient to meet the objectives of the network code on cybersecurity?

○ Yes ◉ No opinion ○ No

If your answer is "No", what could be improved?

Title VII: HARMONISING PRODUCT AND SYSTEM REQUIREMENTS AND VERIFICATION

29. Is the proposed approach for harmonizing the cybersecurity procurement requirements and verification schemes clearly described and sufficient to meet the objectives of the network code on cybersecurity?

○ Yes ○ No opinion ◉ No

If your answer is "No", what could be improved?

The network code must precise the rhythm of the rolling work program (number of requirement sets per year vs number of critical businesses). Without it, the evaluation does not make sense.

The goal of both Art 35 and 36 seems to explain that ENTSO-E and the EU DSO Entity have the right and possibility (though no obligation) to develop non-binding CS procurement requirements and guidance on the union certification schemes. Since none of the articles are meant to create actual obligations, it is not clear why those articles are in the draft NCCS in the first place.

Moreover, the NCCS should make it clear that i) the electricity entities remain free to adopt their own procurement requirements and that ii) the so called non binding procurement requirements cannot bind them in any way.

Harmonising the cybersecurity procurement requirements can or should only be consulting guidelines and not enforced rules. This leaves more flexibility to buy assets in the scope area at the market.

More precise security requirements for suppliers are required, also covering existing MRO contracts.

Title VIII: ESSENTIAL INFORMATION FLOWS INCIDENT AND CRISIS MANAGEMENT

30. Article 37 request CS-NCA to provide electrity entities with information on cybersecurity indicents, threats, and vulnerabilities to enhance the electricity entities' defense. Do you agree that the network code will help electricity entities to receive effective and adequate information to increase their threat awareness and ability to handle cybersecurity incidents?

○ Yes ○ No opinion ◉ No

If your answer is "No", what should be changed in the information sharing process?

The tool presented in paragraph 8 is very interesting and could allow fluid information exchanges to improve communication. We nevertheless would like to share some practical considerations:
Article 37(8) should not merely foresee a feasibility study for the development of an IT tool but rather a) clearly plan for the development of such a tool; b) allocate the responsibility to such a tool on an actor, c) determine key requirements in terms or availability, redundancy, resilience, back-up, functionality and cybersecurity of the tool itself and d) allocate sufficient funding for such a tool.
Art.37 should also provide clearer indications in terms of timing.

In terms of applicability, it should also be clarified when the IT tool needs to be made available and when the obligations relying on the availability of such a tool should start applying. It does not seem appropriate to ask CSIRTs to comply with those obligations if they are not realistically given the means to comply with those. Similarly, it seems important to clarify what should happen in case the IT tools becomes unavailable.
It is important that the reporting requirement is set at a reasonable level so both large companies and smaller companies can manage and adapt the report. Please specify mandatory controls from cross border risk assessment for incident process to be aware of.

31. Article 39 and Article 40 present the support electricity entities receive in the event of an incident (Art.39) and crisis (Art.40). Do you think that enough support is provided?

○ Yes ○ No opinion ◉ No

If your answer is "No", how should the support be reinforced?

Art 39 and 40 foresee that support can be provided the electricity entities. But it is not clear how this support could materialise and it is therefore doubtful that any help would actually be provided.

Incident guidance and support must be clear and practicable. A clear definition is needed when incidents are to be reported, as well as when feedback is given from CSIRT. The use of a standardised common taxonomy for cyber incidents, foreseen in Art 37(7), as Mitre ATT&CK framework can support a rapid and stringent reporting. This allows the recipients of the shared information, to be clear what kind of threat it is.

32. Is the proposed approach for essential information flows and crisis management clearly described and sufficient to meet the objectives of the network code on cybersecurity?

○ Yes ○ No opinion ◉ No

If your answer is "No", what could be improved?

We appreciate the great efforts which have been put into the elaboration of this title to bring a much-needed common framework to share essential information and address incidents and crisis, but we believe that a number of points need further improvement in this title:
i) the title often refers to "CSIRTs" and to "CSIRTs of the Member State" whose roles and responsibilities are different. It however seems that the two terms are sometimes used interchangeably. This must be reviewed to ensure that each actor is vested with the appropriate obligations.
ii) Art 37 allocated obligations on the CS NCA or CSIRT: it should be clearer which actor the obligation is allocated on.
iii) Art 37(4) allows the CS NCA or the CSIRT to assess the level of classification for the information and to inform the entity of the outcome of its assessment: it is not clear against what parameters this assessment is made or what concrete actions could come out of the assessment.
iv) in Art 37(5)(b), who determines the relevant technical information, according to what process and against which criteria?
v) what is the goal and purpose of ENISA's guidance on establishing CSOC capabilities? What happens if it is not followed?
vi) in Art 38(1)(b), it is not clear what the obligation for the electricity entities to "encourage the provision of automated tools including AI" for the CSOC capabilities means.

Questions regarding the proposal on the EU's supranational incident management of cyberattacks. The new proposal contains more far-reaching requirements for incident reporting to CSIRT at EU level. It is extremely important to ensure methodology, but above all the feasibility of reporting and follow-up and reporting to the entities reporting incidents. More questions from the authorities do not always mean that the activities get a better picture of the situation. The new proposal must be manageable for both large companies as well as small energy companies. Reporting requirements will require increased resources; therefore, it is important that the reporting requirement is set at a reasonable level. Gathering information about incidents at an EU body can also pose risks of hacker attacks and leaking knowledge of weaknesses in national systems.

Integration of Switzerland into these processes would make sense for both, EU and Switzerland.

Title IX: ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

33. Article 41 requires critical entities to perform two exercises every three years. Do you have the capabilities to perform the mandatory cybersecurity exercises?

○ Yes ○ No opinion ◉ No

If your answer is "No", how frequently should exercises be held?

These exercises should follow the top down & bottom up approach cycle: two exercises every 4 years (1 exercise every 2 years) could be more appropriate.

We also see challenges in terms of managing resources, financings, and in terms of general coordination:

- For corporate groups where the multiplication of exercises at entity/national level risk straining the availability of CSOCs and CSIRTS
- With critical service suppliers, where the NC CS requires contractual modification to take place with suppliers to require them to take part in the CS exercises.

34. Is the proposed electricity cybersecurity exercise framework clearly described and sufficient to meet the objectives of the network code on cybersecurity?

○ Yes ○ No opinion ◉ No

If your answer is "No", what could be improved?

There are still uncertainties on the proposed electricity cybersecurity exercise framework:

- It is not possible at this stage to have a clear overview of the obligations on the electricity entities in terms of cybersecurity exercises without the definition of the critical processes.
- The key success criteria are not defined for the moment in the NC. The absence of a proper definition does not allow to determine the success of the exercise nor of the remedial actions to be adopted to remedy the vulnerabilities.
- It is not clear for the time being in the NCCS who will produce or contribute to the lessons learnt report, or what would be the governance model for the national or regional cybersecurity exercises.

We believe that it is important to stress that the organisation of all those cybersecurity exercises will require additional funding and that it will have significant financial costs.

Title X: PROTECTION OF INFORMATION EXCHANGED IN THE CONTEXT OF THIS DATA PROCESSING

35. Are the principles and implementation rules for protection of information adequate to protect classified and sensitive information to be exchanged in a trusted way?

○ Yes ○ No opinion ◉ No

If your answer is “No”, which principles and/or implementation rules should be removed, added or modified?

Some work is still required to ensure a robust protection of information:

- In Art 46:

- There are a lot of principles listed in the Art in view of protection the information which needs to be exchanged in the framework of the NC, but without clear indication of what the principles mean in practice nor on who lies the obligation to respect those principles. The Article needs to be redrafted so as to establish clearer obligations with clearly identified addressees.
- Art 46 is not yet actionable and should provide a clearer roadmap to be followed by the actors when handling information. For instance, it should not be for the addressees of the

NCCS to wonder how to ensure their compliance with the already existing other pieces of legislation on data protection (protection of commercially sensitive, confidential information and trade secrets, Regulation (EU) 2016/679 and Regulation (EU) 1227/2011) but the NCCS should provide a framework which ensures that there is no conflict with those other pieces of legislation.

- Art 11, 46, 47 and 48 all require classifying the information. It is not clear whether it relates to the same or different classifications. This needs to be clarified so that stakeholders have only one clear set of obligations to comply with. It seems furthermore that there are inconsistencies in the approach supported, Art 11 focusing for instance on the interests of the information originator whereas Art 46 focuses on the interests of the EU and its Member States. The categories used for the classification of the information diverge also between the articles in the NCCS but also diverge from the classification used in the Commission Decision (EU, Euratom) 2015/444. The coherency and consistency need to be ensured.

- Art 47 only creates an obligation to classify the information in different categories but does not explain what regime applies to those different categories of data. The classification is not sufficient to ensure the application of a legal regime of data protection. This needs to be made more explicit. In the same way, is the possibility for the data originator to "limit distribution, restrict use or indicate releasability" supposed to be binding and if so, what is the interest of the classification of data in the first place? Are the rules of Chapter 4 of the Commission Decision (EU, Euratom) 2015/444 supposed to apply by analogy?

- Art 47 and 48: it is not clear whether both Articles are meant to apply to the information exchanged in the context of Title VIII.

The reporting of inventory assessments and risk assessments included in the processes is governed by national legislation that currently prevents information from being reported to EU. Coherence with current national legislation in this field is important, keeping in mind not to pose additional administrative burden on entities under the scope of CSNC regarding existing reporting obligations.

It is missing how critical information is exchanged (e.g. through a secure platform?).

36. Is the proposed protction of information exchanged in the context of this data processing clearly described and sufficient to meet the objectives of the network code on cybersecurity?
○ Yes ○ No opinion ◉ No
If your answer is "No", what could be improved?

There is not enough reasoning why ACER needs companies' information.
It should be mentioned that the communication needs to be encrypted for TLP red information.

General

37. Do you see any areas where the network code on cybersecurity can be aligned better with the revised NIS directive now under development?
Please elaborate

We have noted after the NIS-2 negotiations (3rd of December); It is in the proposal that the banks be granted an exemption given that the Council has adapted the text to sector-specific legislation, in particular the Regulation on Digital Operational Resilience for the Financial Sector (DORA Regulation) and the Directive on the resilience of critical entities (CER Directive), in order to create legal clarity and ensure coherence between the NIS 2 Directive and these acts. We would like to see the same consideration given to the Clean Energy Package and the Network Codes, there Network Code for Cybersecurity is one of eight codes for the Electricity Sector.

The scope of the network code should be be made more clear so that entities subject to requirements have sight and knowledge at the outset and do not have to wait for a working group to come up with ECII methodologies and thresholds.
The Energy sector face multiple new targets for managing controls and meeting new cybersecurity requirements that must be coordinated both by the EU and nationally by authorities, including the upcoming NIS 2, the Cybersecurity Act, as well as this new regulatory instrument. The regulations must be more coherent and streamlined to each other as far as taxonomy and methods are concerned. We also highlight that the NCCS and the NIS 2 Directive are now elaborated in parallel, whereas the NCCS will have to comply with the framework established by the NIS 2 Directive. Time is needed to ensure better coherency and consistency among both texts.

38. Do you have any other comment you want to share and that are not included in the previous questions, with regard to the draft network code on cybersecurity?
Please elaborate

We welcome the work carried out. Most of the main concepts and ideas are there. However, we believe work should be done to integrate the “gathered risks”: this is a really important topic the network code should tackle. The systemic risk resulting from gathered attacks against several entities with low individual risk is real. Methodologies should be written to assess and tackle this.

Our concern is that rules on cyber-security will be defined in the network code, but its scope of applicability will remain unclear until either (i) development and implementation of a methodology on risk assessment and defining Electricity Cybersecurity Risk Index (ECRI) or (ii) transitional measures are adopted by the cybersecurity working group. This representants significant uncertainty for the electricity undertakings.
The risk assessments included in the processes are strongly regulated by national law which prevents such information from being reported.
There are doubts about the accountability of the risk management process foreseen by ACER and ENISA. While the cross-border risk assessment process is more inclusive than the transitional process none of the two processes guarantee due accountability. The cross-border risk assessment report will determine obligations of electricity undertakings; however, it is not subject to any regulatory or judicial review.

We recommend that the network code either defines the scope of applicability directly – by listing the electricity undertakings that fall within the scope or indirectly – through setting a methodology determining the applicability. Delegating the competence to define the scope of applicability through an implementation process is likely to result in uncertainty and accountability issues. Please keep in mind the lengthy and complex process of implementing the Network Code Balancing.

Derogations from NCCS: It is not clear under what circumstances derogations will be possible, especially for countries that have already implemented some cyber requirements but are unsure

whether they conform or not. The process of checking and reporting this should be kept as simple and easy as possible.

The framework and process for Risk Assessment and rating of entities is unclear. Hence, it is very difficult to foresee the implications of NCCS on a country and its enterprises. Please clarify how this process (including timelines) is foreseen and what are the responsibilities of the different actors in the process (NRA, Ministries, enterprises, cybersecurity bodies, etc.)

Eurelectric pursues in all its activities the application of the following sustainable development values:

Economic Development

- Growth, added-value, efficiency

Environmental Leadership

- Commitment, innovation, pro-activeness

Social Responsibility

- Transparency, ethics, accountability

Union of the Electricity Industry - Eurelectric aisbl
Boulevard de l'Impératrice, 66 – bte 2 - 1000 Brussels, Belgium
Tel: + 32 2 515 10 00 - VAT: BE 0462 679 112 • www.eurelectric.org
EU Transparency Register number: 4271427696-87